UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/389,437	09/03/1999	SULTAN WEATHERSPOON	5038-12	5396

20575 7590 05/06/2005

MARGER JOHNSON & MCCOLLOM, P.C.
1030 SW MORRISON STREET
PORTLAND, OR 97205

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/389,437	WEATHERSPOON ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 remain for examination.

Response to Arguments

2. In view of the appeal brief filed on 8/11/04, PROSECUTION IS HEREBY REOPENED. New grounds for rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 2 recites the limitation "the second authentication message" in line 3. There is insufficient antecedent basis for this limitation in the claim. In view of the second authentication message recited in claim 3, Examiner interprets its appearance in claim 2 to be a typographical error. Appropriate correction or clarification is required.

5. Claim 15 recites the limitation "the control channel" in line 2. There is insufficient antecedent basis for this claim. Although a control channel is declared in claim 14, claim 15 does not depend on that claim, and thus it is unclear if the respective control channels are intended to be the same. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-4, 6-12, and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dynarski et al. (U.S. Patent 6,466,571).

Referring to claims 1 and 9:

Dynarski discloses a secure LAN comprising a wireless device coupled to a wireless device operator (element 14 of Figure 1A), an access point coupled to the wired computer LAN in communication with the wireless device through an air channel to authenticate the wireless device without going through a firewall (the system illustrated by element 40 of Figure 1A, and col. 6, lines 5-30), and an authentication server coupled to the wired computer LAN to provide the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator without going through the firewall (element 28 of Figure 1A, and col. 5, lines 35-55).

Although Dynarski does not disclose a firewall, it does disclose a router that controls access to the wired LAN from the outside (element 22 of Figure 1A). It is also well known in the art that routers can perform the duties of a firewall to prevent unauthorized traffic into a secured LAN (see the Windows NT TCP/IP Administration reference cited below for an illustration). Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to add firewall capabilities to the gateway router disclosed by Dynarksi. The motivation would be to limit access to the wired LAN from the outside to authorized sources only.

Regarding claim 16:

Dynarksi teaches a method for operating a local area network comprising:

- Generating a first authentication message including validating information about an access point connected to a wired LAN (col. 7, lines 55-61);
- Transmitting the first authentication message from the access point to a wireless device over a wireless channel (Ibid)
- Validating the access point by analyzing the first authentication message without going through a firewall means (col. 7, line 62 – col. 8, line 10)
- Generating a second authentication message including validating information about a wireless device and a wireless operator (Ibid)
- Transmitting the second authentication message from the wireless device to the access point (Ibid)

- Validating the wireless device by analyzing the second authentication without going through the firewall means (Ibid)
- Transmitting the [first and] second authentication messages to an authentication server after validating the access point and wireless device without going through the firewall means (col. 8, lines 10-20, but see footnote below)
- Validating the operator, the wireless device, and the access point without going through the firewall means (col. 9, lines 25-40)
- Enabling a data channel between the wireless device and other devices on the wired LAN after validating the operator, the wireless device, and the access point without going through the firewall means where validating the access point, the wireless device, and the operator occurs at an authentication means (col. 9, lines 25-40)

With respect to transmitting both messages, the cited passage only indicates that the contents of the second message are forwarded to the authentication server. It would have been obvious to one of ordinary skill in the art at the time the invention was made to forward the first message as well, with the motivation being that it may be beneficial for the authentication server to know what type of service the wireless device will be expected to provide (such as data or voice-over-IP, see col. 7, lines 58-61) in order to allow different permissions for each type of service.

Referring to claims 2, 10 and 17:

Dynarksi teaches or suggests the limitations of claims 1 and 9. Dynarksi also teaches a first authentication device to send a first authentication message to the wireless device, the [first] authentication message including validating information about the access point (col. 7, lines 37-43 and 55-61).

Referring to claims 3, 11, and 18:

Dynarksi teaches or suggests the limitations of claims 2 and 10. Dynarski also teaches a second authentication device to send a second authentication message to the access point, the [second] authentication message including validating information about the wireless device and operator (col. 7, line 62 – col. 8, line 10).

Referring to claims 4 and 12:

Dynarksi teaches or suggests the limitations of claims 3 and 11. Dynarksi also teaches where the access point sends the second authentication messages to the authentication server after authenticating the wireless device (col. 8, lines 10-20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to forward the first message as well, with the motivation being that it may be beneficial for the authentication server to know what type of service the wireless device will be expected to provide (such as data or voice-over-IP, see col. 7, lines 58-61) in order to allow different permissions for each type of service.

Referring to claims 6, 14, and 19:

Dynarski teaches or suggests all the limitations of claims 1, 9, and 16. Dynarksi explicitly teaches that one embodiment of that invention uses the wireless technology described in the Conolly reference (U.S. Patent 5,325,419; see Dynarksi, col. 6, lines 20-25). Conolly teaches that the wireless technology contains a control channel used to send authentication data (col. 12, lines 25-30 and also column 24). Examiner concludes that Dynarksi would also possess a control channel for communication of authentication data between the wireless device and the access point. Even were that not so, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include them, with the motivation being to make the wireless technology backwards compatible with pre-existing wireless technologies that do support a control channel (Conolly, Ibid).

Referring to claim 7:

Dynarksi teaches or suggests the limitations of claim 6. Dynarksi further teaches including a data channel on the wired LAN for sending data from the wireless device to any other device, the data channel being enabled after the authentication message is validated by the authentication server (col. 9, lines 25-40). It should be noted that although the preferred embodiment of the Dynarksi disclosure focuses on ultimately establishing a connection between the wireless device (element 14 of Figure 1A) and a computer on a different LAN (element 10 of Figure 1A, for example), observe that the wireless device is not connected to any IP network, and is therefore inaccessible to any

device *including other computers on the same LAN*, until after the authentication procedure is completed (col. 7, lines 45-60). Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to stipulate that the authentication procedure also be required for the wireless device to send data to any other device *on the same LAN*. Given that the wireless device, being inside any firewall means that may be present on the home router or elsewhere on the link between the LAN and the WAN (element 20 of Figure 1A), need not go through the firewall to access any other computer on its home LAN, then the motivation for the above would be to provide an alternate means of security (in lieu of a firewall) to ensure that only authorized wireless devices access computers on that LAN.

Referring to claims 8, 15 and 20:

Dynarksi teaches or suggests the limitations of claims 6, 13, and 16. Dynarksi explicitly teaches that one embodiment of that invention uses the wireless technology described in the Conolly reference (Dynarksi, col. 6, lines 20-25). Conolly teaches that communications between the wireless device and the access means over the control channel are encrypted (Conolly, see column 24). Therefore, it is deemed inherent to the Dynarksi disclosure that encryption of traffic over the control channel between the wireless device and the access point are encrypted. Even were that not so, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include it, with the motivation being that sending unencrypted authentication

information would make it very easy for an attacker to compromise in order to gain unauthorized access to the system, thus defeating the purpose of the invention.

8. Claims 5 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dynarksi as applied to claims 3 and 11 above, and further in view of "Apply Personal Mobility in PCS Environment for Universal Personal Communications" by Ling-Sheng Chen (hereinafter "Chen").

Referring to claims 5 and 13:

Dynarski teaches or suggests the limitations of claims 3 and 11. Dynarski is silent regarding the use of smart cards, although it does disclose that the devices contain an International Mobile Subscriber Identity number, or "IMSI" (col. 2, lines 5-10) which is used in the authentication procedure (col. 5, lines 55-65), and that in one embodiment the wireless technology conforms to the PCS standard as taught by Conolly (Dynarksi, col. 6, lines 20-25). However, Chen teaches that one could use smart cards with PCS (Chen, "2. Synergy Between PCS and UPT", 2nd paragraph), and that such cards comprise an IMSI (Chen, "6. Numbering and Identification"). Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use smart cards as the authentication devices used in the invention disclosed by Dynarski. The motivation for doing so would be to facilitate the use of mobile devices on multiple networks (Chen, "1. Introduction", 2nd and 3rd paragraphs; see also Dynarksi, Abstract).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- U.S. Patent 6,600,734 (issued to Gernert et al.)
- U.S. Patent 6,272,129 (issued to Dynarksi et al.)
- U.S. Patent 6,151,628 (issued to Xu et al.)
- U.S. Patent 6,088,337 (issued to Eastmond et al.)
- U.S. Patent 5,737,318 (issued to George A. Melnik)
- U.S. Patent 5,654,959 (issued to Baker et al.)
- U.S. Patents 5,559,886; 5,390,245; and 5,282,250 (issued to Dent et al.)
- Hunt, Craig and Thompson, Robert Bruce. Windows NT TCP/IP Network Administration. O'Reilly & Associates, Inc. © October 1998. [Chapter 12]

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
4/15/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100